IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Adrian Alvarez Diez
Serial No.:	10/562,488
Filed:	December 22, 2005
Group Art Unit:	2458
Confirmation No.:	6307
For:	METHOD AND SYSTEM FOR AUTHENTICATING SERVERS IN A DISTRIBUTED APPLICATION ENVIRONMENT

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF IN SUPPORT OF APPEAL
FROM THE PRIMARY EXAMINER TO THE BOARD OF APPEALS

This is an appeal of a Final Rejection of claims 1-19 of Application Serial Number 10/562,488 filed December 22, 2005. This brief is being submitted pursuant to 37 C.F.R. 1.192. A Notice of Appeal was filed on June 11, 2009.

The appeal brief fee of $540.00 is:

☐ Enclosed.

☐ $40 required. ($500 paid in prior appeal.)

☒ Charged to Deposit Account No. **<u>09-0465</u>**.

Table of Contents

1. Real Party in Interest

International Business Machines Corporation is the real party in interest.

2. Related Appeals and Interferences

There are no related appeals or interferences pending with this application.

3. Status of Claims

Claims 1-19 are pending. The Final Office Action rejecting claims 1-19 was mailed on March 11, 2009.

Appellant appeals from the final rejection of claims 1-19. The claims on appeal are set forth in Appendix A.

4. Status of Amendments

No amendments were filed subsequent to the Office Action mailed on March 11, 2009.

5. Summary of Claimed Subject Matter

Appellant is appealing from the Examiner's rejection of claims 1-19. Claim 1 is an independent claim. Claims 2-6 and 17 depend directly or indirectly from claim 1. Claim 7 is an independent claim. Claims 8-11 depend directly or indirectly from claim 7. Claim 12 is an independent claim. Claims 13-15 and 18 depend directly or indirectly from claim 12. Claim 16 is an independent claim. Claim 19 depends directly from claim 16.

Claim 1 is directed at a method for authenticating a third tier server system in a distributed application environment (e.g., *abstract, ¶ [0017]).* The distributed application environment comprises a client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and third tier server system which exchanges data between said client system and said server systems *(e.g., ¶ [0017]; Figs. 2A, 4-5).* The client system acts as single point of recognizing and managing third tier server certificates and provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment *(e.g., ¶¶ [0044]-[0047], [0070]).* Claim 1 further requires that, at said server systems side, the method comprise:
receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server *(e.g., ¶¶ [0017], [0044], [0048], [0064]),* comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system *(Id.),* accepting said third tier server system as to be authenticated if said at least all necessary information matches said server-copy of the third tier certificate *(Id.)*

***Claim** 7* is directed at a method for authenticating a third tier server system in a distributed application environment (e.g., *abstract, ¶ [0017]).* The distributed application environment comprises a client system having parts of the distributed

application, server systems having the remaining parts of the distributed application, and a third tier server system which exchanges data between said client system and said server systems *(e.g., ¶ [0017]; Figs. 2A, 4-5).* The client system provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment *(e.g., ¶¶ [0045]-[0047], [0070]).* Claim 7 further requires that, at said client system, the method comprise:
receiving a client-copy of a third tier server certificate from a third tier server system *(e.g., ¶¶ [0017], [0044], [0048], [0064]),* determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy *(Id.),* storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy *(Id.),* and transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server system *(Id).*

Claim 12 is directed at a system for authenticating a third tier server system in a distributed application environment (*e.g., abstract, ¶ [0017]).* The distributed application environment comprises a client system having parts of the distributed application,-and application server systems having the remaining parts of the distributed application *(e.g., ¶ [0017]; Figs. 2A, 4-5).* Claim 12 further requires the application server systems-comprise a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system (*e.g., ¶ [0042]; Fig. 2C, element 120),* a connection negotiator component which, in a second computer process receives incoming third tier server certificates via a secure connection between said application server systems and said third tier server (*e.g., ¶ [0038]; Fig. 2C, element 140),* and a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client *(e.g., ¶ [0039]; Fig. 2C, element 130).*

Claim 16 is directed at a client system for authenticating third tier server in a distributed application environment(e.g., *abstract, ¶ [0017]).* The distributed application environment comprises a client system having parts of the distributed application, application server systems having the remaining parts of the distributed application *(e.g., ¶ [0017]; Figs. 2A, 4-5).* Claim 16 further requires that the client system comprise a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server *(e.g., ¶ [0028], Fig. 2B, element 60)*, a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment *(e.g., ¶ [0032]; Fig. 2b, element 4)*, a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common database if it matches *(e.g., ¶ [0029], Fig. 2B, element 50)*, a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base *(e.g., ¶ [0030]; Fig. 2B, element 40)*, and a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection *(e.g., ¶ [0031]; Fig. 2B, element 30).*

6. Grounds of Rejection to be Reviewed on Appeal

The Examiner has rejected claims 12-16 under 35 U.S.C. § 101, as directed to non-statutory subject matter. Accordingly, the first issue is whether claims 12-16 are statutory subject matter.

The Examiner has rejected claims 1, 4-9, and 16-17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication 2002/0152382 (hereafter *Xiao*) in view of Appellant's Background Section (hereafter *Background Section*). The Examiner has also rejected claims 2-3, 10-15, 18, and 19 under 35 U.S.C. § 103(a) as being unpatentable over Xiao in view of Background Section and further in view of U.S. Patent 6,233,577 (hereafter Ramasubramani). Accordingly, the second issue is whether the Examiner is correct in asserting these combinations obviate claims 1-19.

7. Argument

I. Rejections under Section 101

The Examiner rejected claims 12-16 under 35 U.S.C. § 101 because the server and client components could be implemented in software alone. Appellant respectfully asserts that, irrespective of the Examiner's assertion, the claims are still patentable because satisfy the "machine" prong first articulated in the recent Federal Circuit *Bilski* decision. More specifically, claim 12 is directed at an application server in a distributed application environment, comprising:

> a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system,
>
> a connection negotiator component which, in a second computer process receives incoming third tier server certificates via a secure connection between said application server systems and said third tier server, and
>
> a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client.

Claim 16 is similarly directed to a specific machine, namely a client system for authenticating third tier server in a distributed application environment comprising:

> a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server,
>
> a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment,
>
> a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common data base if it matches, and
>
> a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base,
>
> a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being

> accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection.

The Examiner appears to concede that claims 12 and 16 satisfy the *Bilski* test, but believes that that this test is only applicable to "method" claims. *Office Action mailed March 11, 2009 at pg. 14; Advisory action mailed May 26, 2009.*

Appellant respectfully traverses. First, the Examiner's *per se* refusal to consider the *Bilski* test appears to be inconsistent with the current Patent Office practice; this Appeal Board has frequently applied the *Bilski* machine-or-transformation analysis to "apparatus" claims. *See* AIPLA Electronic and Computer Law Committee, *Post-Bilski Subject Matter Eligibility Opinions* 72-115 (June 14, 2009), *citing as examples e.g., Ex parte Godwin*, Appeal No. 2008-0130 (B.P.A.I. Nov. 13, 2008); *Ex parte Uceda-Sosa*, Appeal No. 2008-1632 (B.P.A.I. Nov. 18, 2008); *Ex parte Nawathe*, Appeal No. 2007-3360 (B.P.A.I. Feb. 9, 2009).[1] Second, Appellant respectfully submits that the Examiner's position is internally inconsistent. The Examiner rejects claims 12-16 because they could be implemented as software, but then refuses to accept the applicability of the Federal Circuit's recent cases on the patentability of software-implemented inventions. Third, Appellant submits that there is no legal or policy reason for subjecting the inventions in claims 12-16 to a more ***stringent*** test merely because the inventions are defined as an 'apparatus.' The Examiner has conceded that similar method claims are patentable. If similar claim language is statutory as a "method," it should also be statutory when defined as a specific "apparatus."

[1] Currently available at http://www.aipla.org/Content/Microsites106/Electronic_and_Computer_Law2/Subcommittee_Pages/Patents_and_Legislative_Affairs/cases-4-101.pdf?CFID=3813440&CFTOKEN=24006989

II. Rejections under section 103

The Examiner bears the initial burden of establishing a prima facie case of obviousness. *MPEP 2141.* Establishing a prima facie case of obviousness begins with first resolving the factual inquiries of *Graham v. John Deere Co.* 383 U.S. 1 (1966):

(A) determining the scope and content of the prior art;

(B) ascertaining the differences between the claimed invention and the prior art'

(C) resolving the level of ordinary skill in the art; and

(D) considering any objective indicia of nonobviousness.

Once the *Graham* factual inquiries are resolved, the Examiner must then determine whether the claimed invention would have been obvious to one of ordinary skill in the art.

A. Claim 1

Appellant respectfully submits that the Examiner has not properly characterized the teachings of the references and/or the claims at issue, and thus, has not established the prima facie case of obviousness. More specifically, Appellant respectfully asserts that neither of the references cited in this case teaches or suggests "at said server systems side said method comprises receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server" and "comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system."

The primary reference, Xiao, is directed as a "server-based certificate management system that delivers certificates and associated trust information to clients to verify received certificates." Xiao, ¶ *[0050].* In this system, the server sends its server certificate to the client. *Xiao at* ¶ *[0074].* The client then hashes the server certificate, and then compares the result hash with a list of trusted entity 'thumbprints' stored in a 'trusted information object.' *Id. at* ¶ ¶ *[0074]-[0076].* Xiao also describes updating the trusted information object via HTTP, or broadcast. *Id. at* ¶ ¶ *[0081]-[0090].* Significantly, however, the certificate management is done at the server. Xiao even emphasizes that server-side key management is its "key" improvement. *Xiao, [0053] and [0061].*

The invention in claim 1, in contrast, is generally directed at a method for authenticating a third tier server system in a distributed application environment. As noted in Appellant's specification at paragraph [0025], a "significant difference to the prior art is that no database for the certificates at the server side is needed anymore." Appellant's specification goes on to state that a major enhancement compared to the prior art is that "[n]o local certificate database exists on the server systems. Certificate verification is processed exclusively by means of the certificate information sent by the client system. There is no need to administer any third tier certificates locally on the server systems." *Id. At ¶ [0049] (element numbers removed).*

This distinction is specifically reflected in the claim language; claim 1 recites "at said server systems side said method comprises receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server" or "comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system." Xiao, in contrast, specifically teaches that the certificate management should perform at the server side, and not at the client side.

Not only does Xiao fail to teach or suggest these elements, Xiao teaches directly away from them and the claimed invention. As previously noted, Xiao expressly states that its "key" improvement over the art is server-side key management. *Xiao, [0053] and [0061].* The present invention, in contrast, is trying to solve the problems with server-side key management. Because of this divergence, Appellant asserts that there would be no motivation to make the proposed combination.

The Examiner specifically relies on Xiao [0088] and Xiao [0050] as teaching these elements, analogizing the TIO to the claimed common database and also citing various blocks in Figure 2. *Office Action mailed March 11, 2009 at pg. 3.* In response, Appellant respectfully submits that, even assuming this analogy is legitimate, Xiao still fails to meet the claim language. The TIO in Xiao is not "receiv[ed]" ***from*** the client system" "at said server system[]," as claimed in claim 1. It is received ***at*** the client system. Similarly, the ***server*** in Xiao does not "compar[e] said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system" or "accept[] said third tier server system as to be authenticated if said at least all necessary information matches said server-copy of the third tier certificate." The activities described with reference to Xiao, figure 2 are all happening on the ***client*** side. *E.g., Xiao [0053], [0061], and [0075].*

For the sake of completeness, Appellant respectfully asserts that its Background section also fails to teach or suggest these claim elements. Appellant's background section identifies as a drawback that "[e]ach server application has a local certificate database which means additional effort to maintain and to protect the certificate data." The third reference, Ramasubramani, also fails to teach or suggest these elements. Instead, Ramasubramani is also merely directed to a two-tier system where the client and server can send each other their certificates. The Examiner also does not appear to contest either of these assertions.

B. Claims 7, 12, and 16

Claims 7, 12, and 16 contain limitations similar to those discussed with respect to claim 1. Therefore, for the reasons discussed above, Appellant respectfully submits that the proposed combinations also fail to teach or suggest all claim elements, and that there would be no motivation to make the proposed combinations.

C. Claims 2-6, 8-11, 13-15, and 17

These claims are dependent on claims 1, 7, 12, or 16. Accordingly, for the reasons discussed above, Appellant respectfully submits that the proposed combinations also fail to teach or suggest all claim elements, and that there would be no motivation to make the proposed combinations.

8. Claims Appendix

1. Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and third tier server system which exchanges data between said client system and said server systems, wherein said client system acts as single point of recognizing and managing third tier server certificates and provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said server systems side said method comprises:

receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server,

comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system,

accepting said third tier server system as to be authenticated if said at least all necessary information matches said server-copy of the third tier certificate.

2. Method according to claim 1, wherein said at least all necessary information from said client system is received via a non-continuous client-server connection.

3. Method according to claim 2, wherein said non-continuous client-server connection is using a secure transmission protocol.

4. Method according to claim 1, wherein said at least all necessary information consists essentially of a client-copy of said third tier server certificate as stored in the

common data base of said distributed application environment, and a server name which has transmitted said client-copy of said third tier server certificate to said client system.

5. Method according to claim 1, wherein said at least all necessary information consists essentially of a fingerprint of a client-copy of said third tier certificate, and a server name which has transmitted said client-copy of said third tier server certificate to said client system.

6. Method according to claim 1, wherein said at least all necessary information consists essentially of two different fingerprints of a client-copy of the third tier server certificate, a server name which has transmitted said client-copy of the third original tier server certificate to said client system, and a certificate name.

7. Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising a client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and a third tier server system which exchanges data between said client system and said server systems, wherein said client system provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said client system said method comprises:

receiving a client-copy of a third tier server certificate from a third tier server system,

determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy,

storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy, and transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server system.

8. Method according to claim 7, wherein said storing additionally includes storing a name of said third tier server system that has transmitted said client-copy of said third tier certificate.

9. Method according to claim 7, wherein said client-copy of said third tier server certificate is received via a secure transmission protocol.

10. Method according to claim 7, wherein said at least all necessary information is transmitted to said each server of said server systems via a non-continuous secure connection.

11. Method according to claim 8, wherein authentication of said client system is accomplished by user ID and/or password.

12. System for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprises a client system having parts of the distributed application,-and application server systems having the remaining parts of the distributed application, wherein said application server systems-comprise:

a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system, a connection negotiator component which, in a second computer process receives incoming third tier server certificates via a secure connection between said application server systems and said third tier server,

a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client.

13. System according to claim 12, wherein said certificate information comprises two different fingerprints of the original third tier server certificate, name of the server which has transmitted said third tier server certificate to said client system, and certificate name.

14. System according to claim 13, wherein said two different fingerprints are generated by applying two different algorithms to said third tier server certificates received from said common database.

15. System according to claim 14, wherein said application server systems further include the same algorithms as used for generating said two different fingerprints.

16. Client system for authenticating third tier server in a distributed application environment, said distributed application environment comprises a client system having parts of the distributed application, application server systems having the remaining parts of the distributed application, said client system comprising:

a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server,

a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment,

a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common database if it matches,

a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base, and

a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection.

17. Computer program product stored in the internal memory of a computer, containing parts of software code to execute the method in accordance with claim 1 if the product is run on the computer.

18. System according to claim 15, further comprising a client system comprising:

a connection negotiator component for receiving incoming third tier server certificates via a secure connection from said third tier server,

a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment,

a certificate verifier component for comparing received third tier server certificate with information stored in said common database and storing them into said common database if it matches,

a user interface component allowing to reject or accept an unknown third tier server certificate not contained in said common data store, and a certificate transmitter component for extracting all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmitting them to said server systems via a secure connection.

19. System according to claim 16, further comprising an application server system comprising:

a transfer server component supporting non-continuous and secure client-server connection,

a connection negotiator component for receiving incoming third tier server certificate via a secure connection between said server systems and said third tier server,

a certificate verifier component for comparing said third tier server certificate received from said third tier server with said information received from said client system for determining to accept or to reject third tier server, and

a third tier server which exchanges data between said client system and said server.

9. Evidence Appendix

There is no evidence attached for this appeal.

10. Related Proceedings Appendix

There are no related proceedings. Therefore, there are no copies of decisions rendered by a court of the Board attached here.

For each of the foregoing reasons, Appellant submits that the Examiner's final rejections of claims 1-19 were erroneous, and respectfully requests reversal of these decisions.

Respectfully submitted,

Date: August 11, 2009

By: __________________________

Grant A. Johnson
Registration No.: 42,696
IBM Corporation - Department 917
3605 Highway 52 North
Rochester, Minnesota 55901-7829

Telephone: (507) 253-4600
Fax No.: (507) 253-2382